

CLAIMS

What is claimed is:

1. A method, comprising:
initializing a virus scanner during a pre-boot phase of a computer system;
scrubbing data read from an input/output (I/O) device of the computer system
by the virus scanner using a virus signature database before the data is loaded; and
enacting a platform policy if a virus is detected in the data.
2. The method of claim 1, further comprising scrubbing contents of a memory
device of the computer system during the pre-boot phase by the virus scanner.
3. The method of claim 1, further comprising updating the virus signature
database with updated virus signatures.
4. The method of claim 3 wherein the virus signature database is updated
during the pre-boot phase.
5. The method of claim 1 wherein the virus signature database is not exposed to
an operating system executing on the computer system.

6. The method of claim 5 wherein the virus signature database is stored in a firmware-reserved area.

7. The method of claim 1 wherein the virus scanner is executing in a virtual machine monitor (VMM) executing on the computer system, the VMM supporting at least one virtual machine (VM) executing on the computer system.

8. The method of claim 7 wherein scrubbing data read from the I/O device includes:

receiving a request from a requester to read data from the I/O device, the requester in a VM of the at least one VM;

loading at least a portion of the requested data into a buffer;

scrubbing the at least a portion of the requested data with the virus scanner;

returning an error signal to the requester if the virus scanner detects a virus in the at least a portion of the requested data; and

forwarding the requested data to the requester if the virus scanner does not detect a virus in the at least a portion of the requested data.

9. The method of claim 1 wherein the virus scanner is operable during the pre-boot phase, an operating system (OS) runtime phase, and an after-life phase of the computer system independent of an operating system of the computer system.

10. The method of claim 1 wherein the virus scanner scrubs the data without having knowledge of a file system of the data.

11. The method of claim 1, further comprising enacting the platform policy if the virus scanner detects non-normal behavior within the computer system.

12. An article of manufacture comprising:

a machine-accessible medium including a plurality of instructions which when executed perform operations comprising:

initializing a virus scanner during a pre-boot phase of a computer system;

scrubbing contents of a memory device of the computer system during the pre-boot phase by the virus scanner using a virus signature database;

scrubbing data read from an input/output (I/O) device of the computer system by the virus scanner using the virus signature database before the data is loaded;
and

generating an error signal if a virus is detected by the virus scanner.

13. The article of manufacture of claim 12, further comprising receiving updated virus signatures at the computer system to update the virus signature database.

14. The article of manufacture of claim 12 wherein the virus signature database is stored in a place not exposed to an operating system of the computer system.

15. The article of manufacture of claim 12 wherein the virus scanner to be operable during the pre-boot phase, an operating system (OS) runtime phase, and an after-life phase of the computer system independent of an operating system of the computer system.

16. The article of manufacture of claim 12 wherein the virus scanner to scrub the data without having knowledge of a file system of the data.

17. The article of manufacture of claim 12 wherein scrubbing data read from the I/O device includes:

- launching a virtual machine monitor (VMM), the virus scanner to operate from the VMM; and

- launching a virtual machine (VM) to be supported by the VMM.

18. The article of manufacture of claim 17 wherein execution of the plurality of instructions further perform operations comprising:

- receiving a request from a requester in the VM to read data from the I/O device;

- loading at least a portion of the requested data into a buffer;

- scrubbing the at least a portion of the requested data with the virus scanner;

- returning an error signal to the requester if the virus scanner detects a virus in the at least a portion of the requested data; and

forwarding the requested data to the requester if the virus scanner does not detect a virus in the at least a portion of the requested data.

19. The article of manufacture of claim 12 wherein the plurality of instructions to operate substantially in compliance an Extensible Firmware Interface (EFI) specification.

20. A computer system, comprising:

a processor;

a memory device operatively coupled to the processor;

a storage device operatively coupled to the processor; and

at least one flash memory device operatively coupled to the processor, the at least one flash memory device including firmware instructions which when executed by the processor perform operations comprising:

initializing a virus scanner during a pre-boot phase of a computer system;

scrubbing contents of the memory device during the pre-boot phase by the virus scanner using a virus signature database;

scrubbing data read from the storage device by the virus scanner using the virus signature database before the data is loaded in the memory device; and

generating an error signal if a virus is detected by the virus scanner.

21. The computer system of claim 20, further comprising a network interface operatively coupled to the processor, the virus scanner to scrub data read from the network interface using the virus signature database before the data is loaded in the memory device.

22. The computer system of claim 20 wherein the virus signature database is stored in a firmware reserved area of the storage device, the firmware reserved area not exposed to an operating system of the computer system.

23. The system of claim 20 wherein execution of the firmware instructions further perform operations comprising updating the virus signature database with updated virus signatures downloaded from an external virus signature repository communicatively coupled to the computer system.

24. The computer system of claim 20 wherein the virus scanner is operable during the pre-boot phase, an operating system (OS) runtime phase, and an after-life phase of the computer system independent of an operating system of the computer system.

25. The computer system of claim 20 wherein the virus scanner to scrub the data without having knowledge of a file system of the storage device.

26. The computer system of claim 20 wherein the firmware instructions to operate substantially in compliance with an Extensible Firmware Interface (EFI) specification.

27. A computer system, comprising:

a virtual machine monitor (VMM) to support at least one virtual machine (VM);

an input/output (I/O) device, the VMM to emulate an I/O controller for the I/O device;

a virus scanner within the VMM to scrub data read from the I/O device before the data is loaded; and

a virus signature database to facilitate identification of a virus by the virus scanner.

28. The computer system of claim 27 wherein the virus scanner is operable during the pre-boot phase, an operating system (OS) runtime phase, and an after-life phase of the computer system independent of an operating system of the computer system.

29. The computer system of claim 27 wherein the virus scanner to scrub the data without having knowledge of a file system of the I/O device.

30. The computer system of claim 27 wherein the VMM and the virus scanner to operate substantially in compliance with an Extensible Firmware Interface (EFI) specification.